What is claim d is:

1. A method for protecting data generated by a keyboard, comprising the steps of:

reading data from a keypad of the keyboard;

encrypting the read data; and

transmitting the encrypted data from the keyboard to a computer.

2. The method of claim 1 further comprises the steps of receiving the transmitted encrypted data by the computer; and

decrypting the received encrypted data by the computer.

3. The method of claim 1 wherein the step of transmitting comprises the step of using a wireless link over which the encrypted data is transmitted.

4. The method of claim 1 wherein the step of encrypting comprises the step of using an encryption seed; and

entering the encryption seed via the keypad.

5. The method of claim 1 wherein the step of encrypting comprises the step of using an encryption seed; and

receiving the encryption seed from at least one of the computer or a server.

6. The method of claim 1 wherein the step of

encrypting comprises the step of using an encryption seed; and

reading the encryption seed from a device reader connected to the keyboard.

7. The method of claim 6 wherein the step of reading the encryption seed comprises the step of enabling the device reader with a personal identification number.

8. The method of claim 1 wherein the step of encrypting comprises the step of receiving a start signal.

9. The method of claim 8 wherein the step of receiving the start signal comprises the step of generating the start signal by at least one of a special key on keyboard, multi-actuation of a number of keys on the keypad, the computer, or a server.

10. The method of claim 1 wherein the step of encrypting comprises the step of receiving a stop signal that stops the encryption.

11. The method of claim 10 wherein the step of receiving the stop signal comprises the step of generating the stop signal by at least one of a special key on keyboard, multi-actuation of a number of keys on the keypad, the computer, or a server.

12. The method of claim 1 further comprises the step of defining operations of the step of encrypting from program information received from at least one of a device

reader, the computer, or a server.

13. A method for protecting by a computer data generated by a keyboard where the keyboard is connected to the computer, comprising the steps of:

receiving encrypted data from the keyboard by the computer; and

decrypting the encrypted data.

14. The method of claim 13 wherein the step of decrypting comprises the step of performing operations of decryption by at least one of a keyboard driver executing on the computer or an application executing on the computer.

15. The method of claim 13 wherein the step of decrypting comprises the step of using a seed.

16. The method of claim 15 wherein the step of using comprises the step of reading the encryption seed from a device reader connected to the computer.

17. The method of claim 16 wherein the step of reading the encryption seed comprises the step of enabling the device reader with a personal identification number.

18. The method of claim 13 further comprises the step of generating a start signal to cause the keyboard to start encrypting data.

19. The method of claim 13 further comprises the step of generating a stop signal to cause the keyboard to

stop encrypting data.

20. The method of claim 13 further comprises the step of transmitting program information to the keyboard to define encryption operations.

21. A method for protecting by a server data generated by a keyboard where the keyboard is connected to the server via a network and a computer, comprising the steps of:

receiving encrypted data from the keyboard by the server; and

decrypting the encrypted data.

22. The method of claim 21 wherein the step of decrypting comprises the step of performing operations of decryption an application executing on the server.

23. The method of claim 21 further comprises the step of generating a start signal to cause the keyboard to start encrypting data.

24. The method of claim 21 further comprises the step of generating a stop signal to cause the keyboard to stop encrypting data.

25. The method of claim 21 further comprises the step of transmitting program information to the keyboard to define encryption operations.

26. A keyboard for encrypting data before

transmission to a computer connected to the keyboard via a link, comprising:

an interface connected to the link;

a memory;

a keypad for generating the data;

a processor for encrypting the generated data by execution of an encryption routine stored in the memory; and

transmitting the encrypted data to the computer via the interface and link.

27. The keyboard of claim 26 wherein the link is a wireless link.

28. The keyboard of claim 26 comprises a device reader for reading a device to obtain a seed for the encryption routine.

29. The keyboard of claim 26 comprises the processor executing a control routine to receive the encryption routine from at least one of the computer or a server and to store the received encryption routine in the memory.

30. The keyboard of claim 26 comprises a special key which when actuated causes the processor to at least start executing the encryption routine or stop executing the encryption routine.

31. A processor-readable medium for protecting data generated by a keyboard, comprising processor-

executable instructions configured for:

reading data from a keypad of the keyboard;

encrypting the read data; and

transmitting the encrypted data from the keyboard to a computer.

32. The processor-readable medium of claim 31 wherein the transmitting comprises using a wireless link over which the encrypted data is transmitted.

33. The processor-readable medium of claim 31 wherein the encrypting comprises using an encryption seed; and

entering the encryption seed via the keypad.

34. The processor-readable medium of claim 31 wherein the encrypting comprises using an encryption seed; and

receiving the encryption seed from at least one of the computer or a server.

35. The processor-readable medium of claim 31 wherein the encrypting comprises using an encryption seed; and

reading the encryption seed from a device reader connected to the keyboard.

36. The processor-readable medium of claim 35 wherein the reading the encryption seed comprises enabling the device reader with a personal identification number.

37. The processor-readable medium of claim 31 wherein the encrypting comprises receiving a start signal.

38. The processor-readable medium of claim 37 wherein the start signal is generated by at least one of a special key on keyboard, multi-actuation of a number of keys on the keypad, the computer, or a server.

39. The processor-readable medium of claim 31 wherein the encrypting comprises receiving a stop signal that stops the encryption.

40. The processor-readable medium of claim 39 wherein the the stop signal generated by at least one of a special key on keyboard, multi-actuation of a number of keys on the keypad, the computer, or a server.

41. The processor-readable medium of claim 31 further comprises receiving processor-executable instructions for the encrypting from at least one of a device reader, the computer, or a server.

42. An apparatus for executing the steps of claim 1.

43. An apparatus for executing the steps of claim 2.

44. An apparatus for executing the steps of claim 4.

45. An apparatus for executing the steps of claim 5.

46. An apparatus for executing the steps of claim 6.

47. An apparatus for executing the steps of claim 9.

48. An apparatus for executing the steps of claim 12.